YUI KEE

銳基電腦顧問有限公司

Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

September 2009

Contents

Contents 1
Apache Releases Incident Postmortem 1
Paypal Hong Kong Neglects Customer Security 2
Pigeon Beats ADSL 3
Police Apologise to Techie Suspect 3
Politics, Spam and Surveillance 3

Apache Releases Incident Postmortem

<web-link for this article>

The Apache Software Foundation has released a report that describes how attackers broke into various systems, ending with the Foundation downing most of their production servers on August 28th while recovery took place.

The attackers gained access to a server owned by the ApacheCon conference production company and use the SSH key of the backup account to gain access to a staging server and introduce a CGI script to production webservers that was used to obtain remote shells. Fortunately, largely because of defence-in-depth strategies, Apache Software Foundation code repositories, downloads, and users were not put at risk by the intrusion.

The report is instructive in that it provides a detailed picture of how an attacker can eploit weaknesses, and also for Apache's unflinching analysis of their strengths and weaknesses. High points were the use of ZFS snapshots that allowed speedy restore of a known-good state, redundant services in two locations and diversity in the server operating systems that made it difficult for the attackers to escalate privileges on multiple machines. Low points were mis-management of SSH keys, an rsync setup that allowed undetected introduction of files to production servers, CGI scripting enabled on hosts where it was not needed, and keeping log files on the initially-compromised server that allowed the attackers to destroy the evidence of their entry method.

Apache's openness and transparency extend to more than their source code.

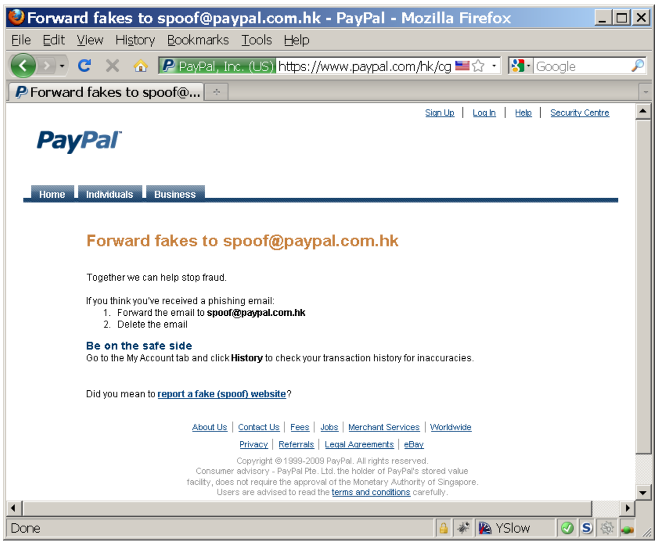
More Information

apache.org incident report for 8/28/2009
Breaching Fort Apache.org - What went wrong?
Hackers scalp Apache
apache.org downtime - initial report
Apache.org Hack

Paypal Hong Kong Neglects Customer Security

<web-link for this article>

Allan Dyer


Forward fakes to spoof@paypal.com.hk - PayPal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
PayPal, Inc. (US) https://www.paypal.com/hk/cg
Google
Forward fakes to spoof@...
Sign Up | Log In | Help | Security Centre
PayPal
Home Individuals Business
Done
YSlow

Forward fakes to spoof@paypal.com.hk

Together we can help stop fraud.

If you think you've received a phishing email:

1. Forward the email to **spoof@paypal.com.hk**
2. Delete the email

Be on the safe side
Go to the My Account tab and click **History** to check your transaction history for inaccuracies.

Did you mean to report a fake (spoof) website?

About Us | Contact Us | Fees | Jobs | Merchant Services | Worldwide
Privacy | Referrals | Legal Agreements | eBay

Copyright © 1999-2009 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd. the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

A recent incident has highlighted poorly-designed procedures and policies at Paypal Hong Kong. On 7th September 2009, I, a Paypal customer in Hong Kong, received a message, supposedly from Paypal. My suspicions were immediately aroused: the message was in Traditional Chinese, a language I cannot read, and Paypal has my language preferences on record. I checked the Paypal website, and forwarded the message to the address for reporting phishing attempts, spoof@paypal.com.hk. However, I also thought it possible that it was a genuine message, but Paypal disregards the needs of "minority" customers. Looking further, I noticed that the message included my name registered with Paypal, a feature included because it is difficult for bulk emailers to guess the correct names for each phishing message, but also that the message arrived from the mailserver om-paypal-apac.rsys4.com [12.130.139.51]. The domain rsys4.com is registered to RESPONSYS Inc., 900 Cherry Avenue, 5th Floor, San Bruno, CA 94066, US, not to Paypal.

Intrigued, I called the Paypal Hong Kong hotline (35508574) and spoke to their customer service officer Nicky. She indicated that phishing emails should be forwarded to spoof@paypal.com, and I would get a response in three to four days, and that spoof@paypal.com.hk was not the correct address. She was uncertain what happened to emails sent to the address listed on the Paypal website.

I therefore asked Nicky to investigate what happened to three earlier phishing reports I made to spoof@paypal.com.hk, on 22 January 2009, 9 May 2009 and 6 August 2009, that had received no response. To facilitate future communications, I asked for the tracking number of this incident, but was told that they do not use tracking numbers. So:

- The Paypal website lists the address for reporting phishing emails as spoof@paypal.com.hk, on the page https://www.paypal.com/hk/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/antiphishing/PPPhishingReport-outside.
- The Paypal customer service hotline in Hong Kong says that the address for reporting phishing emails is spoof@paypal.com, and there should be a response in three to four days.
- There has been no Paypal response to three reports made more than a month ago.
- The Paypal customer service hotline in Hong Kong does not issue incident tracking numbers.

With the current confusion between the Paypal website, and the Hong Kong customer service; and the lack of response on earlier incidents, it is clear that Paypal can make some improvements in how it handles customers and security.

More Information

Forward fakes to spoof@paypal.com.hk
Paypal Language Features Inconvenience Users

Pigeon Beats ADSL

<web-link for this article>

A pigeon beat a Telkom ADSL line in the transfer of 4GB of data across 70Km near Durban, South Africa. The pigeon, called Winston, tweeted in flight. IPoAC or CPIP (RFC1149) was used, making this the largest data transfer using the protocol reported.

Reports did not specify if any protection against H5N1 was used.

More Information

At the speed of a Bird?
Virus Risks of RFC1149 and RFC2549
Pigeon beats Telkom
Winston the Pigeon
The Pigeon
Pigeon beats Telkom

Police Apologise to Techie Suspect

<web-link for this article>

An incident reported by this newsletter four years ago has finally ended, with an apology from the London Police. David Mery, computer and telecoms enthusiast and former editor of EXE was arrested in July 2005 for suspicious behaviour including wearing a rucksack containing a laptop and fiddling with a mobile while waiting for the tube. Since then, he has campaigned for justice, liberty and a critical examination of the "profiling" techniques that led to his arrest. Finally, he has received a letter of apology from the Commander of the Police resonsible, Chief Superintendent Wayne Chance:

> *I would like to apologise on behalf of the Metropolitan Police Service for the circumstances that arose on 28 July 2005 including your unlawful arrest, detention and search of your home. I appreciate this has had a deep and traumatic impact on your lives and I hope that the settlement in this case can bring some closure to this.*
>
> *I shall ensure that the officers concerned are made aware of the impact of the events of that day and also the details of the settlement in this case.*

David Mery also wrote a guide on how innocent people can get their DNA profile deleted from the British Police's National DNA Database (NDNAD).

More Information

Panicky Plod apologises to Innocent Terror Techie
Profiling for Terrorists Catches Techie
How to delete your DNA profile
Innocent in London – 'Suspicious behaviour on the tube'

Politics, Spam and Surveillance

<web-link for this article>

Allan Dyer

This newsletter is not intended to promote a party political agenda, but, by advocating the use of technology in society, particularly when related to information security, there are times when there is overlap of areas of interest with Political Parties and elected politicians. Cases include discussions on the Unsolicited Electronic Messages Ordinance (UEMO) and several privacy leak incidents. A recent email from the Hong Kong Liberal Party raises questions in both these areas, and also official language policy.

It is important to note that the message, sent on 23rd September, by design or by fortuitous accident, does not contravene Hong Kong's laws. It is exempt from the provisions of the UEMO because it is a non-commercial message, an exemption I argued against, and, because it was sent to our webmaster address, it was not addressed to a particular person so it is not covered by the Personal Data Privacy Ordinance. The message, sent only in Traditional Chinese, was apparently a survey of SMEs concerning the introduction of minimum wage legislation. If it had been a commercial message, I would have reported it to OFTA for multiple breaches of the UEMO:

- Suspicion of address generation of address harvesting. "Webmaster" is a well-known address for reporting website issues, and is published on our website for that purpose. Other email addresses are published there for other contact purposes. As a human entering addresses would have chosen a more suitable address, it therefore seems likely that the address was either automatically generated, or harvested by automatic means, both activities prohibited for commercial messages by the UEMO.
- Failure to provide an unsubscribe facility.
- Failure to provide accurate sender information in English and Chinese

The message also contained a webbug, potentially tracking when the message was opened, and a misleading link, labelled as leading to the Liberal Party website, but actually leading to a third-party tracking site. If the message had been sent to a personal address, which perhaps others sent in the same batch were, it might have contravened these Data Protection Principles:

- Principle 1 -- Purpose and manner of collection This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject. The message gave no warning that opening it, or using the misleading link, would result in a record of that activity, linked to the recipient's email address, being recorded.
- Principle 5 -- Information to be generally available This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used. The message, and the website, do not have a Privacy Policy.

On receiving the message, I decided to ask the Liberal Party about these issues, sending an email to them:

> *Dear Liberal Party*
>
> *I have received a message, apparently from you, concerning SMEs and the minimum wage. Unfortunately, the text is only in Traditional Chinese, that I cannot read. As a registered voter in Hong Kong and a Director of an SME, I would like to ask the following questions:*
>
> 1. *What is your party's position on the official languages of Hong Kong? How do your actions support that position?*
> 2. *How did you obtain the email address webmaster@yuikee.com.hk? What is your party's position on the Unsolicited Electronic Messages Ordinance, in particular, the provisions on harvesting of email addresses?*
> 3. *Your message contains a link that appears in the text as "http://www.liberal.org.hk/", but which actually goes to the location "http://crm.astamarketing.com/liberal/EmailMgr/CampClickThroughTracker.amx?campaignUrlId=3D45D04D9EE0DABD22C8DA3D1790D57D92&mailContactRecordId=3D48BD5223DA39C0B9191B682F896997A9&campaignDeliveryId=3D70B4853B3BADD4D22BB444E5AE263752", also, the bottom of your message has an image that is loaded from the URL*

> > *http://crm.astamarketing.com/liberal/EmailMgr/CampOpenTracker.amx?campaignDeliveryId=3D70B4853B3BADD4D22BB444E5AE263752&mailContactRecordId=3D48BD5223DA39C0B919 1B682F896997A9*
> >
> > *This is apparently an attempt to monitor without notification or consent which recpients of the message opened it, and which clicked through the link. What is the policy of your party on monitoring the activities of individuals without notification and consent?*
>
> *I look forward to your detailed reply.*
>
> *Regards*
> *Allan Dyer*

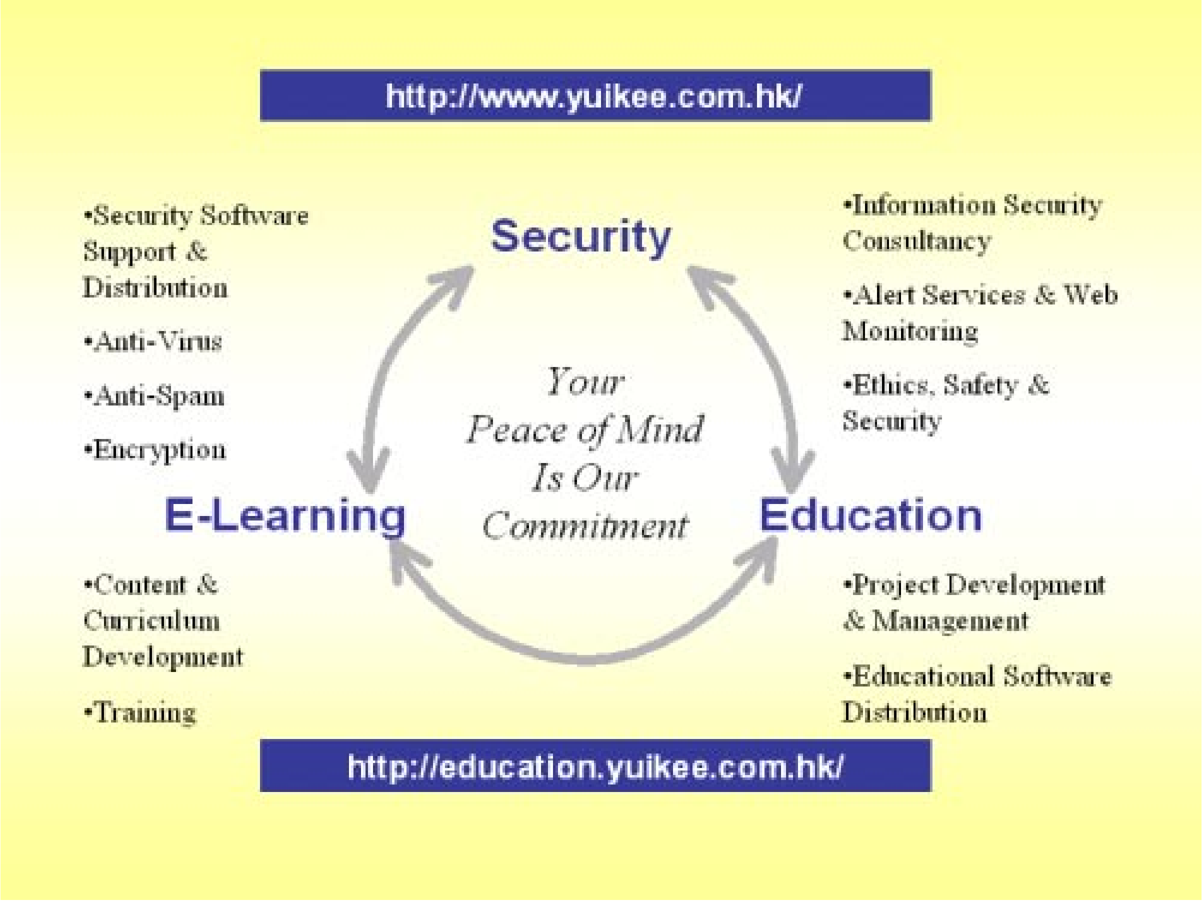
Staff at the Liberal Party confirmed on 23rd September that they had received the message and would reply to it. A response has not been received at the time of writing this article.

More Information

Response to the UEM Proposals
Liberal Party (自由黨) Official Home Page
Privacy Commissioner tells Mobile Operator to Improve Website Security
Data Leak Disease
Is Hong Kong's new Anti-Spam Law Effective?
Data Protection Principles

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

Security

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/